第4回　DSK-IDC メルマガ

テレワークの突貫工事に STOP ！
見落としがちなセキュリティを
無料診断中！

今回はテレワークを急遽導入した企業が見落としがちな、セキュリティ対策の重要性と弊社のセキュリティ無料診断をご紹介いたします。

あなたの会社はテレワークを導入されましたでしょうか。コロナウイルスの影響で一部地域では緊急事態宣言が発令され、目標としてテレワークを導入し会社に出勤する社員を７割減らすことが求められています。しかし、急遽テレワークを導入したことで、セキュリティ対策がおろそかになっている企業が多く見受けられます。

自分の会社はサイバー攻撃とは無縁と思われている方が多いですが、サイバー攻撃に企業の規模は関係なく、全ての企業がサイバー攻撃の対象になります。

では、どのような情報がサイバー攻撃のターゲットとなるのでしょうか、それは社員の個人情報や顧客情報です。サイバー攻撃によって流出したデータが顧客情報であれば、企業の信用が失われ、損失は計り知れません。

「セキュリティ対策の重要性は分かったけれど何から始めればよいか分からない」と思われた方の為に、サイバーセキュリティチェックリストをご用意いたしました。以下にチェックリストを少しお見せします。

ご回答内容

運用面

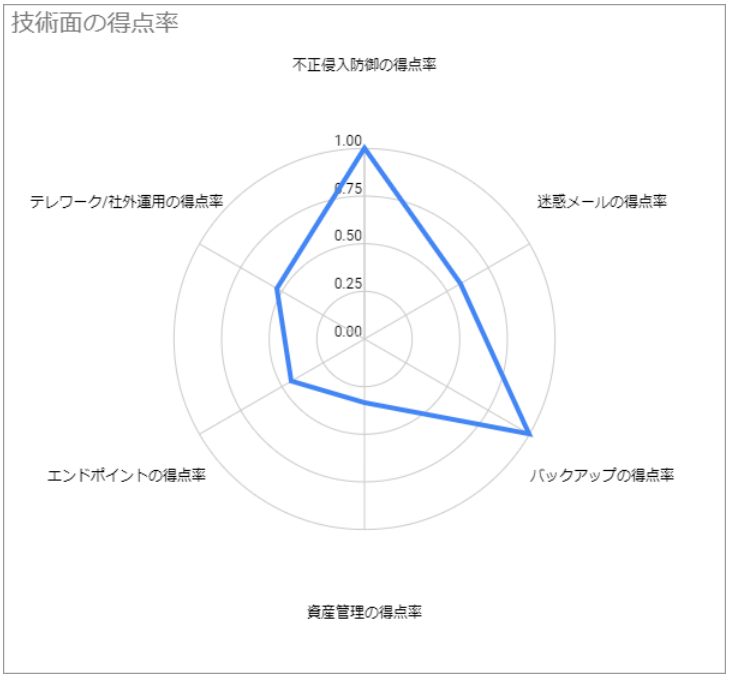
		実施している	一部実施している	実施していない	わからない
No.1	御社のパソコンや会社支給のスマホなど、情報機器の OS やソフトウェアは常に最新の状態にしていますか？			○	
No.2	御社のパソコンや会社支給のスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※は最新の状態にしていますか？	○			
No.3	パスワードは破られにくい「長く（10 桁以上）」「複雑な（英字大小＋数字＋記号）」パスワードを設定していますか？		○		

チェックリストにチェックしていただければ、弊社が診断レポートを作成させていただきます。チェックリストは専門家が考察することで初めてサイバーセキュリティの課題を発見できます。弊社にはセキュリティアドバイザーと呼ばれるサイバーセキュリティの専門家がおり、彼らから最適なサイバーセキュリティ対策をご提案させていただきます。ぜひこの機会にテレワークのセキュリティを見直しされてみませんか。

次のページに、セキュリティ診断結果のサンプルを掲載いたします。
セキュリティ診断してみたいと思われた方は、以下の Web サイトよりお問い合わせください。

https://www.dsk-idc.jp

3. 技術面の評価



評価点数　65 / 100 点

インターネットへの入口、出口の対策やバックアップ対策はできておりますが、資産管理やファイアウォール以降の内部機器の対策が不十分で、社内端末がマルウェア感染してしまった場合に、途中で感染の拡大を阻止できず業務がストップしてしまう危険があります。

【各項目についての評価】

不正侵入防御 (100 / 100 点)		不正侵入防御の対策はできているようです。
迷惑メール (58 / 100 点)		メールのセキュリティ対策が不十分です。サイバー攻撃はメールからの感染脅威がトップです。マルウェア感染や標的型攻撃のターゲットにされてしまう危険があります。
バックアップ (100 / 100 点)		重要情報の消失に備えてバックアップ対策はできているようです。
資産管理 (33 / 100 点)		IT資産管理の対策が不十分です。ソフトウェアライセンス違反などのコンプライアンス違反や、端末台数、パッチ適用状況が把握できていないことによるセキュリティ低下の危険、余剰コストに気づけない危険があります。
エンドポイント (44 / 100 点)		エンドポイントセキュリティ対策が不十分です。マルウェアが未然に防止できない危険や、脅威が可視化されていないことによる対応の遅延が起こりえます。
テレワーク (53 / 100 点)		テレワークや社外利用時のセキュリティ対策が不十分です。外部から社内ネットワークへの不正アクセスの危険や情報漏えいの危険があります。